

### **REMARKS/ARGUMENTS**

Claims 4–13, 15–16, 18–22, and 27–30 remain in the present application, of which claims 4, 11, 15, 16, and 18–22 are independent. Claims 4, 6, 10, 11, 12, 13, 15–16, and 18–22 are amended herein. Claims 27–30 are newly added. Claims 1–3, 14, 17, and 23–26 are cancelled without prejudice. Applicants respectfully request reconsideration and allowance of claims 4–13, 15–16, 18–22, and 27–30.

Applicant thanks the Examiner for indicating that claims 4–9 are allowable if amended to incorporate the underlying elements of their base claims. As such, claim 4 has been amended to incorporate the elements of underlying claims 1 and 2. Claims 5–9 depend, directly or indirectly, from claim 4. Thus, Applicants believe that claims 4–9 (as well as the remaining claims) are in condition for allowance.

### **Information Disclosure Statement**

The IDS filed on June 10, 2005 was objected to because it allegedly failed to comply with the rules. A new IDS is attached hereto, including a copy of the cited foreign patent document cited therein.

### **Objections to the Specification**

The specification was objected to because it did not include an abstract, and it was allegedly improperly arranged. An appendix is included following page 14 of this response including an abstract on a separate sheet.

To further prosecution, Applicants have amended the specification to include the following:

1. Insert “BACKGROUND” before ¶ [0001];
2. Insert “SUMMARY” between ¶¶ [0005] and [0006];
3. Insert “BRIEF DESCRIPTION OF THE DRAWINGS” between ¶¶ [0026] and [0027];  
and

**Appln No. 10/538,449**  
**Amdt date October 8, 2008**  
**Reply to Office action of July 8, 2008**

4. Insert “DETAILED DESCRIPTION OF EXEMPLARY EMBODIMENTS” between ¶¶ [0030] and [0031].

A further appendix is attached with a clean version of the specification including the above amendments for the Examiner’s reference (not intended to be a replacement specification). In light of these amendments Applicants respectfully request the objections to the specification be withdrawn.

**Objections to claims 1, 4, 11, 15–17, 20, and 24**

Claims 1 and 24 are cancelled herein.

Claims 4, 11, 15–17, and 20 were objected to due to a variety of informalities. Applicants have amended each of these claims to properly include transitional phrases, to include antecedent bases, and to correct grammatical errors, as the Examiner requested. Thus, Applicants respectfully request that the objections to the claims be withdrawn.

**Objections to the Drawings**

The drawings were objected to because they allegedly failed to comply with the rules, and reference characters 21 and 31 were unclear. The specification has been amended to replace an instance of the reference number 31 with the number 21, as noted above, in ¶ [0074]. Applicants believe this amendment resolves the objections to the drawings provided in the paragraphs numbered 9 and 10 on page 4 of the Office action.

**Claim Rejections under 35 USC § 112**

Claims 25–26 were rejected under 35 U.S.C. § 112, second paragraph, as allegedly being indefinite in that they fail to point out what is included or excluded by the claim language. Claims 25–26 have been cancelled without prejudice.

**Claim Rejections under 35 USC § 101**

**Appln No. 10/538,449**  
**Amdt date October 8, 2008**  
**Reply to Office action of July 8, 2008**

Claims 1–3 were rejected under 35 U.S.C. § 101 because the claimed invention allegedly lacks patentable utility. Claims 1–3 have been cancelled without prejudice.

**Claim Rejections under 35 USC § 102**

Claims 1–3, 10–12, 14–26 were rejected under 35 U.S.C. § 102(b) as allegedly being anticipated by Naccache (EP 0578059 A1). Claims 1–3, 14, 17, and 23–26 have been cancelled without prejudice. Applicants respectfully traverse the anticipation rejections of claims 10–12, 15–16, and 18–22.

Claim 10 depends from claim 4, which the Examiner has indicated is allowable as amended to include the limitations of its underlying claims. Thus, claim 10 incorporates all the terms and limitations of claim 4 in addition to other limitations, which together further patentably distinguish these claims over the art of record. Therefore, Applicants request that the rejection of claim 10 be withdrawn and that this claim be allowed.

In the anticipation rejections of the Office action, the Examiner makes numerous assertions that do not appear to be supported by the Naccache reference, only a few of which are cited below for brevity.

In rejecting claims 11, 19, 20, and 22, for example, the Examiner asserts that Naccache discloses “providing to the verifier device a value  $s^e$  being the Montgomery  $e^{\text{th}}$  (i.e.  $d$ ) power of  $r$  (i.e.  $D$ ) where  $r$  is a random number, and transmitting the value of  $x$  to the verifier device.” However, this portion of Naccache discloses that “the prover device computes and sends  $\underline{U = r * B^d D^d \bmod n}$  to the verifier device.” (Underlining added for emphasis.) The Montgomery  $e^{\text{th}}$  power of a random number  $r$ , as claimed in claim 11, is not the same as the equation cited in Naccache. Many other limitations of claim 11, and also used in the rejections of claims 19, 20, and 22, are similarly not disclosed in Naccache.

In rejecting claims 18 and 21, the Examiner apparently uses the limitations of claim 4, and, for example, asserts that Naccache discloses “providing to the verifier device a value  $v = s^2$

being the Montgomery multiplication of the secret number  $s$  (i.e.  $B$ ) by itself (page 4, lines 16–17).” However, this portion of Naccache discloses that “The basic relationship between the secret key  $B$  and a user’s (prover device) identity is:  $f(ID)*B^v = 1 \bmod n$ . Another short name for  $f(ID)$  is  $J$ . The parameter  $v$  is decided by the authority.” This portion appears wholly unrelated to the claimed limitation. Many other limitations of these claims, used in the rejections of claims 18 and 21, are similarly not disclosed in Naccache.

In rejecting claims 15 and 16, for example, the Examiner asserts that Naccache discloses on page 3, lines 25–30, “means for computing the Montgomery product of  $y = r x_m s$ ,” where  $r$  is a random number,  $x_m$  is the Montgomery representation of the Montgomery square of  $r$ , and  $s$  is a secret number. However, this portion of Naccache discloses an equation that appears unrelated, which does not include a Montgomery square of a random number. Many other limitations of these claims, used in their rejections, are similarly not disclosed in Naccache.

For at least these reasons, each of the independent claims is believed to be allowable and not anticipated by Naccache, because Naccache does not disclose at least one limitation of each of the independent claims.

Furthermore, because claim 12 depends from claim 11, and claims 27–30 depend from claims 4 or 11, respectively, they each incorporate all the terms and limitations of their respective independent claim in addition to other limitations, which together further patentably distinguish these claims over the art of record. Therefore, Applicants request that the rejection of claims 12 and 27–30 be withdrawn and that these claims be allowed.

### **Claim Rejections under 35 USC § 103**

Claim 13 was rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Naccache as applied to claim 11 above, and further in view of Brickell (US Patent 7,165,181 B2). Applicants respectfully traverse.

Applicants submit that the embodiments of the invention as claimed in claim 13 are not taught, described or suggested in Naccache, even in view of Brickell. Claim 13 depends from claim 11. Brickell does not supply the deficiencies of Naccache discussed above with respect to

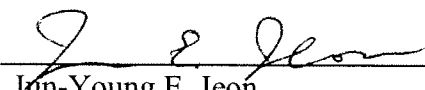
**Appln No. 10/538,449**  
**Amdt date October 8, 2008**  
**Reply to Office action of July 8, 2008**

the anticipation rejection of claim 11, so there is no apparent reason why a person having ordinary skill in the art would have combined the cited references to arrive at the claimed invention of claim 13.

**Concluding Remarks**

In view of the foregoing amendments and remarks, Applicant earnestly solicits a timely issuance of a Notice of Allowance with claims 4–9. If there are any remaining issues that can be addressed over the telephone, the Examiner is cordially invited to call Applicant's attorney at the number listed below.

Respectfully submitted,  
CHRISTIE, PARKER & HALE, LLP

By   
Jun-Young E. Jeon  
Reg. No. 43,693  
626/795-9900

JEJ/sc

SC PAS808721.2.\*-10/8/08 10:31 AM